РАЗРАБОТКА АЛГОРИТМА ВОССТАНОВЛЕНИЯ ИСХОДНОГО СОСТОЯНИЯ ПРОГРАММ

канд. техн. наук,доц. С.Ю. Гавриленко, магистр В.В. Челак, студент Е.В. Челак, Национальный технический университет "Харьковский политехнический институт", г. Харьков

На сегодняшний день существуют целые семейства вредоносных программ, которые маскируются путем внедрения в программное обеспечение (ПО) [1, 2]. Одной из задач антивирусных программ являться восстановление исходного состояния инфицированного ПО. Принцип восстановления базируется на деактивации вредоносного кода, который заключается в замене вредоносных фрагментов кода на команды *пор*, которые предписывают ничего не делать. Такой подход приводит к изменению сигнатуры файла. Так, например, хеш-сумма SHA-1 исходного ПО, зараженного и восстановленного с помощью Dr.Web и AVG имеет 4 разных хеш-кода. (табл.)

Таблица – Сравнение SHA-1 для 4 видов одного ПО

Файл	SHA-1	Размер
Исходный	90765f3688eb286332e2f8fcce73211bc167ef30	667,5 Кб
Зараженный	581d9e042e7a2169d6b0a3453368bd2eb52c5df6	694 Кб
Лечение Dr.Web	319b99899767947be01067aedec7cd8467fc2d44	677 Кб
Лечение AVG	5760ea57d41dcae52d12054e265e35ebd196b9cc	667,5 Кб

Как результат, восстановленные файлы воспринимаются антивирусными системами как вредоносное программное обеспечение, несмотря на удаление вредоносных сигнатур

В работе предложен алгоритм восстановления исходного состояния инфицированного ПО, при котором достигается полное совпадение с исходной сигнатурой файла. Алгоритм базируются на определении способа заражения. В зависимости от способа заражения выполняется удаление вредоносных фрагментов кода (безусловных переходов в тело вируса, тело вируса).

Полученные результаты показали возможность использования данного алгоритма для восстановления исходного состояния ПО от вредоносного программного обеспечения семейства Virus (подсемейство Virut).

Список литературы: **1.** *Касперски К.* Искусство дизассемблирования / *К. Касперски, Е. Рокко*. – СПб.: БХВ-Петербург, 2008. – 896 с. **2.** *Гошко С.В.* Технологии борьбы с компьютерными вирусами / *С.В. Гошко*. – М.: Солон-Пресс, 2009. – 352 с.